

What is claimed is:

1. A detection system for identifying and eliminating excessive requests for information on a network to prevent the failure of a portion of the network, comprising:
at least one switching device, wherein the switching device has predefined parameters for the receipt of an acceptable volume of requests for information;
5 at least one server, wherein the switching device and server are in electronic communication with each other; and wherein the switching device is configured to receive requests for information and attempts to respond to the request; and
an activity monitoring system, the activity monitoring system comprising a route arbiter and a traffic analyzer, wherein the activity monitoring system is in electronic
10 communication with the switching device.
2. A detection system as claimed in claim 1, further comprising a firewall, wherein the firewall is configured to receive requests for information.
3. A detection system as claimed in claim 1, wherein the route arbiter monitors the requests received by the router.
4. A detection system as claimed in claim 2, wherein the route arbiter is coupled to the firewall and the switching device, and wherein the route arbiter monitors the requests received by the firewall and the switching device.
5. A detection system as claimed in claim 1, wherein the route arbiter is configured to compare the volume of requests to the predefined parameters for the receipt of an acceptable volume of requests.

6. A detection system as claimed in claim 1, wherein the route arbiter is configured to instruct the switching device to direct requests for information to the traffic analyzer.

7. A detection system as claimed in claim 1, further comprising a null address router, wherein the null address router is coupled to the traffic analyzer.

8. A method for preventing the failure of a first network device on a network, wherein the network has a network address that is broadcast, and wherein the first network device is configured to receive a predefined volume threshold of packets of information from a second network device, comprising:

5 the first network device receiving repeated packets of information from the second network device, wherein the second network device identifies the first network device by the network address;

monitoring the volume and frequency of the transmitted packets of information;

10 determining whether the volume of transmitted packets of information exceeds the predefined threshold of acceptable volume of transmission of packets of information;

directing the transmission of packets of information from the second network device to an analyzer;

analyzing the transmission of packets of information at the traffic analyzer; and

15 responding to the forwarding of the packets of information from the second network device.

9. A method as claimed in claim 8, wherein responding to the forwarding of packets of information further comprises instructing the first network to cease advertising the network address to the second network device.

10. A method as claimed in claim 8, wherein responding to the forwarding of packets of information further comprises forwarding the packets of information from the analyzer to a null address router.

11. A process for identifying and preventing the failure of a network device on a first network having a plurality of first network devices, wherein the first network is coupled to a second network via at least one edge router, the second network having a plurality of second network devices, and wherein the first network comprises a core router, a server having a server network address, a route arbiter, and a traffic analyzer, and wherein the core router announces the server network address to the second network and first network devices, comprising:

predefining a parameter for an acceptable volume of traffic from a transmitting source;

receiving a first volume of traffic at the core router, wherein the volume of traffic is transmitted from a first source;

monitoring the first volume of traffic by the route arbiter;

determining whether the first volume of traffic exceeds the predefined parameter of an acceptable volume of traffic from a transmitting source;

if the first volume of traffic exceeds the predefined volume parameter, instructing the core router to direct the first volume of traffic from the first source to the traffic analyzer;

analyzing the first volume of traffic to determine whether the volume is decreasing; and

responding to the excessive volume of traffic.

12. A process as claimed in claim 11, wherein responding to the excessive volume of traffic comprises instructing the router to cease announcing the server network address to the first source.

13. A process as claimed in claim 11, wherein responding to the excessive volume of traffic comprises directing the traffic from the first source to a null address router.

14. A method for determining the best connection or path for a router to transmit traffic to a specific destination on a network, wherein a path on a network includes a plurality of independent segments that are coupled together via links, and wherein the volume of users on the network defines the network load, comprising:

- 5 analyzing the amount of network load; and
- analyzing link availability to determine the specific links to traverse, wherein the analysis of link availability comprises:
 - analyzing traffic load on the specific link pathway, wherein the traffic load is the volume of users on the specific link; and
 - 10 analyzing the availability of the network.

15. A method as claimed in claim 14, wherein analyzing the traffic load on a specific pathway further comprises transmitting a sample packet from a starting point and measuring the amount of time for the packet to return to the starting point.